Denial of Service Attacks and Challenges in Broadband Wireless Networks

Shafiullah Khan[1,2], Kok-Keong Loo[1], Tahir Naeem[1,2], Mohammad Abrar Khan[1,2]

[1]School of Engineering and Design, Brunel University, London, United Kingdom
[2]Kohat University of Science and Technology (KUST), Kohat, N.W.F.P, Pakistan

Summary
Broadband wireless networks are providing internet and related services to end users. The three most important broadband wireless technologies are IEEE 802.11, IEEE 802.16, and Wireless Mesh Network (WMN). Security attacks and vulnerabilities vary amongst these broadband wireless networks because of differences in topologies, network operations and physical setups. Amongst the various security risks, Denial of Service (DoS) attack is the most severe security threat, as DoS can compromise the availability and integrity of broadband wireless network. In this paper, we present DoS attack issues in broadband wireless networks, along with possible defenses and future directions.

Key words:
Broadband networks, wireless mesh networks, IEEE 802.11 WLAN, IEEE 802.16, Denial of Service

1. Introduction

Broadband wireless networks provide high broadband internet access not only to home users but also to industries and other commodities. Today, broadband wireless networks are the hot topic for businesses, users and researchers. Initially, the cellular networks proved to be revolutionary technologies in the daily life of subscribers, after that the broadband wireless technology of IEEE 802.11 [11] is making progress rapidly. Now the last-mile 802.16 and the integrated technology of WMN are providing high bandwidth solution to the users.

IEEE 802.11 which is also known as Wi-Fi is basically designed to fulfil the broadband requirements of an organization or limited group of users. IEEE 802.11 has replaced the Local Area Network (LAN), therefore it is also known as Wireless LAN (WLAN). The IEEE 802.16 which is also termed as WiMax is Wireless Metropolitan Area Network (WMAN), giving more coverage as compared with the IEEE 802.11. Furthermore, it can be used to connect different WLAN technologies which are apart from each other. WMN is an integrated wireless broadband technology, which not only provide community based city-wide broadband services to end-users, but also integration of other wired and wireless networks such as IEEE 802.11, IEEE 802.16, Cellular, and LANs. The WMN serves as a backbone wireless network for the integration of others.

As these three broadband technologies are providing internet services to hundreds and thousands of end-users, organizations, and other commodities, hence their security is indeed necessary, as secure communication is the key of success for any wireless network especially broadband wireless networks. The internet connectivity adds extra level of security threats and complexities as compared to simple wireless networks. The three important features of a secure wireless broadband network are the confidentiality, data integrity and service availability. The confidentiality is mostly encountered by the passive attacks, integrity is threaten by active attacks, while the availability of the broadband wireless networks are compromised by the most severe form of active attack, i.e. Denial of Service (DoS) attacks. DoS attacks have the ability to bring down an entire broadband wireless networks. therefore DoS is treated as the highest security risk for any wireless network especially broadband wireless networks, as DoS uses the internet as a platform to be launched.

This paper makes four principal findings. First, we compare the three versatile broadband wireless networks. Second, we provide a description of active and passive attacks in broadband networks. Third, we demonstrate the DoS attacks on these technologies. Finally, we introduce some DoS related affects and possible tackling directions.

2. Broadband Networks Architecture Overview

IEEE 802.11 and IEEE 802.16 wireless broadband technologies are difficult to deploy as they need centralized body to control, manage and monitor, and expensive maintenance cost. This is not in the case of WMN, as it is low cost, easily deployable, self-healing and self-configuring decentralized technology. The network architectures of IEEE 802.11, IEEE 802.16 and WMN are different as follows:

Manuscript received July 5, 2008.
Manuscript revised July 20, 2008.

2.1 IEEE 802.11

An IEEE 802.11 is a Wireless Local Area Network (WLAN) technology usually designed to provide wireless network access to an organization or enterprise. The motivation behind this technology was the support of mobile clients within a certain range and to provide wireless network infrastructure in such locations where wired networks are not feasible or possible. The architecture of 802.11 WLAN is given in Fig. 1.

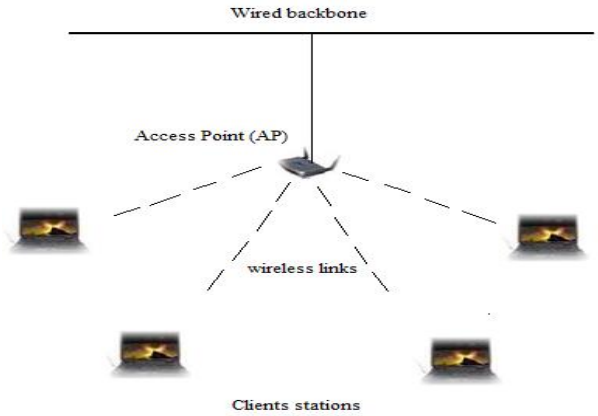

Fig. 1 IEEE 802.11 Architecture

WLAN Consist of two important components, i.e. nodes and an Access Point (AP). The AP provides wireless connectivity to nodes as well as function as a bridge between the nodes and wired network infrastructure. The clients use *Probe request* frames to discover a wireless network, if a wireless network exist then the AP respond with *Probe response* frame. The clients select that AP which provides the strongest signal to it. However, this kind of mechanism may not be optimal if the AP is already overloaded. Here such kind of mechanism are needed which not only consider the signal strength, but also consider the load on AP. If the AP is overloaded then the nodes connect with another nearby AP although the signal strength is relatively weak [4]. Typical applications of WLAN are campus and organizational networking; back haul for public safety and industrial control networks.

2.2 IEEE 802.16

IEEE 802.16 is a Wireless Metropolitan Area Network (WMAN) technology also known as WiMax. This technology offers high bandwidth broadband wireless network and separate levels of services to homes and businesses, i.e. T1 level is for businesses and best effort service level is for home users. It can be used to connect the Wi-Fi hotspots with other parts of the internet, also provide a wireless alternative to fiber optic and other cables for last mile broadband access. The architecture of802.16 WMAN is given in Fig. 2.

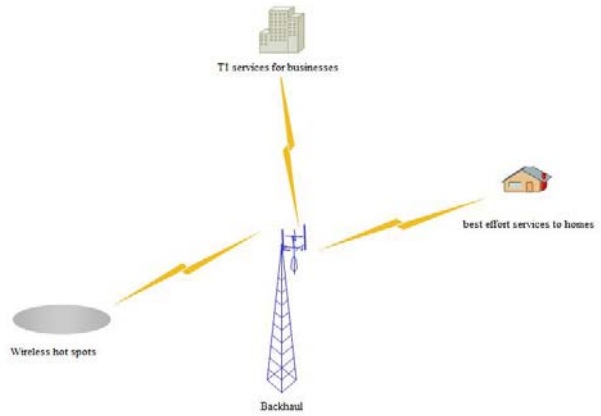

Fig. 2. IEEE 802.16 Architecture

2.3 Wireless Mesh Network

WMN is an emerging 4th generation broadband wireless technology which consists of mesh routers and mesh nodes. The mesh routers form the backbone and provide connectivity to mesh nodes. Some of the mesh routers in WMN perform the functionality of gateways providing internet connectivity to mesh nodes through mesh routers. The nodes in a WMN act both as a client and as a relay router for forwarding traffic for other nodes. In most of the cases, the WMN form partial mesh topology, which means that there are many routes to every node, so if any route is not working then the data traffic can be sent through other route. The architecture of WMN is given in Fig. 3. As early discussed, the main advantages of WMN are its low cost, easy deployment, self healing and self configuring, however, few characteristics of it such as multi-hop nature, dynamic topological changes and the attack prone medium of WMNs are making it more vulnerable to different security threats as compared to IEEE 802,11 and IEEE 802.16.

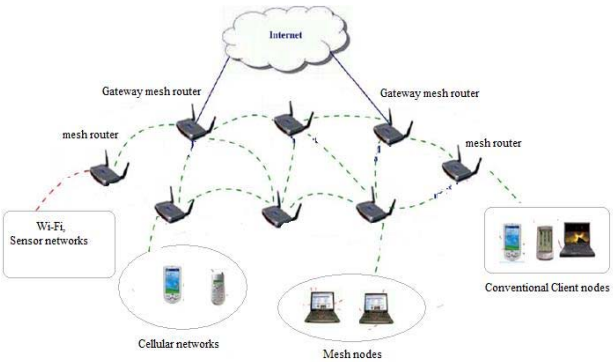

Fig. 3 Wireless Mesh Network Architecture

The characteristics of WMN, IEEE 802.11 and IEEE 802.16 are given in table 1.

Table 1 Characteristics comparison

Characteristic	**IEEE 802.11**	**IEEE 802.16**	**WMN**
Bandwidth	54 Mbps (802.11a)	Up to 70 Mbps	54 Mbps (However decreases with increasing hops)
Coverage	Up to 100 meters	Up to 50 Kilometers	Vey flexible and easily extendable.
Encryption	WEP	56-bit DES, AES	WEP, AES
Authentication	Wi-Fi Protected Access (WPA), WPA 2,	Mobile stations use X.509 certificate to authenticate with Base station	WEP, WPA, WPA2
Transmission	Point to multipoint	Point to point, point to multi-point	Point to multipoint
Deployment Cost	High	Higher	Low
Architecture	Centralized	Centralized	Decentralized
Connectivity basis	Nodes connects with Access Point on the basis of strongest signal	Mobile stations (MS) connect with Base station (BS) on the basis of strongest signal	Mesh nodes connect with wireless mesh routers on the basis of strongest signal; also mesh node can connect with the wireless network through another nearby mesh node.

3. Security Challenges in Broadband Wireless Networks

Today, wireless broadband networks are facing two broad categories of security threats, i.e. passive attacks and active attacks. In passive attacks, the attackers simply analyze and listen to the network traffic with the objective to capture sensitive information of the target. These kinds of attacks compromise the confidentiality of the end user traffic. In passive attack, the unauthorized user gain illegal access to the network traffic without modifying the traffic [13]. Passive attacks are very difficult to detect, as such attacks do not harm the user traffic or normal network operations. However, most of the passive attacks are later used for launching active attacks, as successful passive attack gain information related to the target users, network topology, traffic pattern etc. Such information can later be used for launching active or DoS attack. Passive attacks can be eavesdropping or traffic analysis. WMN is more vulnerable to passive attacks as compared to IEEE 802.11 and IEEE 802.16, as WMN is multi-hop in nature, and the client nodes may have direct ad-hoc connectivity and relay traffic for one another, whereas, IEEE 802.11 and IEEE 802.16 are single hop and there is no ad-hoc type connectivity amongst the nodes.

In the active types of attacks, the attackers have the ability to harm the:

- Network traffic either by tempering, modifications, or dropping the packets
- Broadband wireless network links and established routes between source and destination
- Broadband network resources such as bandwidth
- Produce jitter in transmission and reduce throughput

Again, WMN is more vulnerable to active attacks due to the characteristics of multi-hop and ad-hoc connectivity. As multi-hop nature not only reduce the bandwidth fairness in WMN, but also increases its routing overheads, and most of the attackers exploit these weaknesses and successfully launch active attacks against the WMN. On the other hand, due to less routing overheads and relatively fair bandwidth distribution in single hop wireless broadband networks, it is difficult for the attackers to launch an active attack against them. The harsh form of active attack is DoS attack. The attack types, affect and severity is given in table 2

Table 2. Attacks and severity

Security threats in Broadband wireless networks		
Attack type	Compromise	Severity
Passive attacks	Secrecy Privacy Confidentiality	More severe for end users
Active attacks	Data integrity Service availability	More severe for network and network resources

4. Denial of Service Issues in Broadband Wireless Networks

Denial of Service (DoS) is one of the major issues of all types of wireless networks especially broadband wireless networks. When authorized users are not provided a requested service within a defined maximum waiting time, it means that a DoS violation has occurred [15]. It is the most harmful and dangerous attack which can be launched on any layer of broadband Wireless Network [16]. DoS attacks target availability by preventing communication between network devices or by preventing a single device from sending or receiving traffic [1], where availability ensures that authorized users can access the data, services and network resources from anywhere anytime.

4.1 Physical Layer Vulnerabilities

WMN and IEEE 802.11 uses 2.4 GHz frequency band while IEEE 802.16 uses 10-66 GHz and 2-11 GHz bands at physical layers. DoS attack can be launched against physical layer by using radio jamming device or a source of strong noise to interfere the physical channels and may compromise the service availability. However this kind of attack is not common as it need specialized hardware equipment to be launched, furthermore jamming attacks

can be detected using radio analyzers. It can create great problems during exchange of sensitive information [14] or during warfare. For jamming attack in

- IEEE 802.11, the attacker needs to be close to the target AP
- IEEE 802.16, the attacker needs to be close to the Base Station (BS)
- WMN, the attacker can launch the attack from anywhere.

Due to the vast coverage area and dense deployment of wireless mesh routers in WMN, it is more vulnerable to physical layer DoS attacks.

Currently, IEEE 802.11 uses Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS), IEEE 802.16 is using Orthogonal Frequency Division Multiple Access (OFDM) and Scalable OFDM access (SOFDMA), while WMN uses OFDM and Ultra wide band (UWB) mechanisms for radio transmission. None of the mechanism is capable enough to handle the jamming attack on these broadband wireless networks.

4.2 Link Layer Vulnerabilities

The IEEE 802.11 and WMN MAC uses shared medium amongst the nodes and is highly vulnerable to selfish attack and collisions. The selfish attack improves the bandwidth, throughput and QoS of the selfish node at the cost of another node [12]. An *Attack Detection Model in WMN* is presented in [6], in which a router can blacklist the selfish node ID. CSMA/CA with RTS/CTS mechanism is adopted for IEEE 802.11 and WMN. The current mechanism of CSMA/CA with RTS/CTS can be compromised for MAC layer DoS attack either by sending bulk of MAC control messages to an innocent neighbour or by holding the MAC channel for unnecessary continuous transmission keeping an innocent node back-off [17] The *deauthentication attack* is another form of DoS attack, which is observed in WMN and IEEE 802.11 due to the link layer xvulnerability [5]. The Link layer of IEEE 802.16 is much better as it uses TDMA for uplink and TDM for downlink which ensures collision free transmission.

4.3 Network Layer Vulnerabilities

As compared to IEEE 802.11 and IEEE 802.16, network layer of WMN is highly vulnerable to different DoS attacks due to multi-hop environment, as the number of hops increase the routing overheads increase. DoS attacks at this layer can seriously disrupt the routing mechanism or can degrade the network performance by exhausting network resources. The network layer DoS attacks in WMN can be *Blackhole attack* in which the malicious node absorb all the traffic going toward the target node [10], Greyhole *attack* in which the malicious node selectively forwards the packets to the destination node, *Wormhole attack* to create routing disruptions [3], *Flooding attack* in which the attacker transmits a flood of packets toward a target node or to congest the network and degrade its performance. A flooding DoS attacks are difficult to handle. An active cache based defence against the flooding style of DoS attacks is proposed in [2]; however this mechanism may not be able to handle Distributed DoS attack. All these DoS attacks are observed in WMN due to its multi-hop nature. As the IEEE 802.11 and IEEE 802.16 are single-hop broadband wireless networks, therefore such kind of attacks are not possible in them. It shows that at network layer, IEEE 802.11 and IEEE 802.16 are more secure as compared to WMN.

4.6 Distributed Flooding DoS

A distributed flooding DoS attack is a huge challenge for all the wireless broadband networks, as this attack can bring down an entire network or consume the network bandwidth to a great extent. This kind of attack is launched by first compromising large number of innocent nodes in the wireless network termed as Zombies [9], which are programmed by highly skilled programmer. These zombies send data to selected attack targets such that the aggregate traffic congests the network. In most of the cases, the DDoS is impossible to prevent and it has the ability to flood and overflow the network [7].

In IEEE 802.11 the target of distributed flooding would be Access Point (AP), in WMN the target is wireless mesh router while in IEEE 802.16 it is base station.

4.5 Rogue and selfish backbone devices

The attacker can seriously disrupt the broadband wireless networks by compromising the core network devices. In WMN and IEEE 802.11, a selfish mesh router or selfish AP can degrade the network performance either causing congestion or unavailability. IEEE 802.16, a rogue BS is an attacker station which is used to confuse the mobile stations of the network; as such kind of BS seems and acts like a legitimate BS. Mesh routers or APs are compromised by the attackers using sniffers. A sniffer is an application which is used for passive traffic analysis attack to analyze the network traffic. In IEEE 802.16, the BS is compromised by reprogramming a device with the hardware address of another legitimate device [18]. The hardware address can be detected by intercepting the management messages of IEEE 802.1 using sniffers. The same mechanism can be applied on mesh routers and APs to compromise using hardware address of another network device.

4.6 Authorization flooding on backbone devices

WMN and IEEE 802.11 nodes use *Probe request* frames to discover a wireless network, if a wireless network exist then the AP respond with *Probe response* frame. The clients select that AP which provides the strongest signal to it [4]. Here the attacker can spoof a flood of probe request frames presenting a lot of nodes searching for wireless network, can seriously overload the AP or wireless mesh router. If the load exceeds the threshold value will cause the AP or wireless mesh router to stop responding and may create service unavailability. In IEEE 802.16 the client stations use certificate to authenticate and register with the BS. The client station can send a bulk of registration requests to the BS may result in DoS.

4.7 Node deprivation attack

In node deprivation attack, the attackers target a single node and isolate it from taking part in the normal network operations. In WMN and IEEE 802.11, the nodes first authenticate itself with the mesh router or AP, and needs to de-authenticate [5] it if the node has no more desire to use the network resources. The attacker can spoof the de-authentication message on behalf of the target node so that to stop it from using the network resources. The same vulnerability exist in IEEE 802.16, where the adversary eavesdrop the authentication message exchange between the node and the BS, and then replays this message many times to BS, creating DoS for the target node.

5. Results of DoS Attacks and possible countermeasures

The results of different DoS attacks on broadband wireless networks vary with the nature and type of DoS attack.

- DoS attack is of low intensity, if launched against a single node either to exhaust its battery or to isolate it from the network operations.
- DoS attack is of high intensity if it is launched to make services unavailable for a target area in wireless broadband networks. Selfish mesh router attack in WMN and rogue BS attack is used for this purpose.
- Dos attack will be of highest intensity if it is launched to cripple down the entire broadband wireless network by distributive flooding. Distributed flooding is normally used for this purpose to exhaust the bandwidth of the network or to overflow the resources of the gateways.

DoS in any form against any network is regarded as a severe attack. Some possible countermeasure needs to be investigated to overcome to some extent against DoS and related issues in broadband networks.

- Cognitive radios implementation at physical layer needs to be investigated so that to handle the jamming and scrambling kind of attacks, which are common in all the broadband networks.
- Current encryption mechanisms used in these broadband networks are WEP, DES, and AES, which are vulnerable to eavesdropping kind of attack. Improved and efficient encryption mechanisms needs to be proposed exclusively for each of the broadband technology, as successful eavesdropping later on facilitate the attackers to launch DoS attacks.
- Intrusion detection mechanism can be used to detect and respond to most of the network layer threats particularly for WMN environment.
- A location detection mechanism based on the signal strength needs to be devised for the AP and wireless mesh router with the ability to identify a malicious node for flooding probe request and de-authentication kinds of attacks, same mechanism can be used for the IEEE 802.16 network to identify fake registration request flooding.
- Improved routing protocols are desirable particularly for the multi-hop WMN.

6. Conclusions

In this paper, we discussed the important security issues and different security threats both active and passive risks of important wireless broadband networks. DoS is the severe form of active attack against all types of wireless networks especially broadband networks, and it is capable target a single node, a portion of wireless network, an entire wireless network or wireless network resources. DoS attacks can compromise the two important features of secure wireless networks i.e. data integrity and service availability. WMN is more vulnerable to different types of DoS attacks are compared to IEEE 802.11 and IEEE 802.16 due to multi-hop architecture, vast coverage area, and ad-hoc end-users connectivity. At Physical layer, all the three broadband networks are equally vulnerable to DoS threats, while at Link layer, IEEE 802.16 is relatively more secure. WMN is highly vulnerable to DoS attacks at Network layer due to multi-hop overheads as compared to IEEE 802.11 and IEEE 802.16 which are single-hop having less routing overheads. Keeping in view the importance of WMN, there is a need of such efforts to combat DoS attacks. Cognitive radio design and implementation, improved encryption and authentication mechanisms and exclusive intrusion detection mechanism are possible countermeasures which need to be investigated. More research is needed in securing broadband wireless networks. Only a secure broadband

wireless network will be highly accepted for large scale commercial deployment.

References

[1] D.R. Raymond and S.F. Midkiff, "Denial of service in wireless sensor networks: attacks and defences," IEEE Security and Privacy, Vol.7, No.1, pp. 74-81, March 2008.

[2] L. Santhanam, D. Nandiraju, N. Nandiraju and D. P. Agrawal, "Active cache based defence against DoS attacks in Wireless Mesh Network," Proceedings of the 2nd IEEE Int. Symp.Wireless Pervasive Computing (ISWPC2007), 2007.

[3] F.N. Abdesselam, B. Bensaou and T. Taleb, "Detecting and avoiding wormhole attacks in wireless Ad hoc networks," IEEE Communication Magazine, Vol.46, Issue 4, pp. 127-133, April 2008.

[4] S. Vasudevan, K. Papagiannaki, C. Diot, J. Kurose and D. Towsley, "Facilitating Access Point selection in IEEE 802.11 wireless networks," Proceedings of 5th ACM Conference on Internet Measurement, 2005 .

[5] J. Bellardo and S. Savage, "802.11 Denial-of-service attacks: real vulnerabilities and practical solutions," proceedings of 12th USENIX security symposium, pp. 15-28, August 2003.

[6] H-.G Li, M. Xu and Y. Li, "Selfish MAC layer Misbehavior detection model for the IEEE 802.11-based Wireless Mesh Networks," LNCS 4847, Springer, Heidelberg, pp. 382-391, 2007.

[7] P. Dasgupta, T. Boyd, "Wireless Network Security," Annual Review of Communications, Vol.57, International Engineering Consortium, 2004.

[8] H. Moharrer, "A survey on attacks and countermeasures in mobile Ad Hoc networks". Available at http://ece.ut.ac.ir/Classpages/F86/ECE637/FILES/lectures/security.pdf (accessed July 2008)

[9] G.A Marin "Network security basics," In IEEE Security and Privacy, Vol.3, p 68-72, November 2005.

[10] H-.M. Deng, W. Li, D.P. Agarwal, "Routing Security in Wireless Ad Hoc Networks," IEEE Communication Magazine, Vol. 40, pp. 70-75, October 2002.

[11] T. Tsai and J. Chen, "IEEE 802.11 MAC Protocol over Wireless Mesh Networks: Problems and Perspectives," 19th IEEE International Conference on Advanced Information Networking and Applications, 2005.

[12] L. Guang and C. Assi, "Modeling and analysis of predictable random backoff in selfish environment," ACM 9th International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems, MSWiM 06, October 2006.

[13] [13] T. Karygiannis, L. Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices". NIST Special Publication 800-48, 2002. Available at http://www.governmentsecurity.org/articles/articles2/sp-800-48.pdf_fl/ (accessed July 2008).

[14] M. Barbeau, "WiMax/ 802.16 threat analysis," Proceedings of the 1st International ACM Workshop on QoS and Security in Wireless and Mobile Networks, Q2SWinet, 2005.

[15] V.D. Gligor, "A note on the denial-of-service problem," Proceedings of IEEE Symposium on Research in Security and Privacy, 1983.

[16] X. Gu and R. Hunt, "Wireless LAN attacks and vulnerabilities,"Networks and Communication Systems, 2005. Available at http://www.actapress.com/PaperInfo.aspx?PaperID=19889&reason=500 (accessed July 2008)

[17] Y. Zhang, J. Luo and H. Hu, "Wireless mesh networking, architectures, protocols andstandards," Auerbach Publications, Taylor & Francis Group, First Edition, NY, ISBN: 0849373999, 2006.

Shafiullah Khan is currently a PhD candidate in the School of Engineering and Design, Brunel University, West London, UK. He is also affiliated with the Institute of Information Technology, Kohat University of Science and Technology (KUST), N.W.F.P, Pakistan as a lecturer. His research mainly focuses on wireless broadband network architecture, security and privacy, security threats and mitigating techniques.

Kok-Keong Loo a.k.a. Jonathan Loo received his MSc (Distinction) and PhD at University of Hertfordshire, UK in 1998 and 2003, respectively. Thereafter, he joined the School of Engineering and Design, Brunel University, West London, UK, as a lecturer in multimedia communications. Currently, he serves as a course director for MSc Digital Signal Processing and heads a team of 9 active PhD candidates in the area of multimedia communications. His current research interests include visual media processing and transmission, digital/wireless signal processing, and wireless/broadband network architecture, protocols and securities.

Tahir Naeem is currently a PhD candidate in the School of Engineering and Design, Brunel University, West London, UK. He is also affiliated with the Institute of Information Technology, Kohat University of Science and Technology (KUST), N.W.F.P, Pakistan as a lecturer. His research interest includes wireless/WiMax mesh network quality of service.

Mohammad Abrar Khan is currently a PhD candidate in the School of Engineering and Design, Brunel University, West London, UK. He is also affiliated with the Institute of Information Technology, Kohat University of Science and Technology (KUST), N.W.F.P, Pakistan as a lecturer. His research interest includes multimedia data processing and communications.